BCM One Messaging Service Policies

BCM One, Inc. and its affiliates ("BCM One") have created these Messaging Service Policies ("Policies") in order to provide general guidance regarding your use of BCM One's Messaging Services. There are no warranties in these Policies and these Policies are not inclusive or exhaustive and are subject to change at any time at BCM One's discretion. BCM One reserves the right in its sole discretion to remove or deny any traffic which does not comply with these Policies.

1. **Introduction**. The BCM One messaging solution supports superior quality and high integrity communications. These Policies are designed to promote best practices for exchange of messages. The viability of the messaging ecosystem is dependent on consumer perception of messaging as a trusted and convenient communication environment. These Policies are intended to preserve the credibility and utility of the ecosystem. These Policies are designed to enable wanted messages and prevent unwanted or deceptive messages. Those who violate these Policies may be subject to any penalty set forth below.

2. **Enforcement and Violations**. These Policies will be enforced by both BCM One and its upstream providers. Violations of these Policies may result in affirmative action (including legal action) taken by BCM One and/or its upstream carriers.

3. **Definitions:**
    a. Blacklisting: Numbers which have sent repeated known spam/unwanted content are subject to automatic blacklisting without notification for up to 30 days. Multiple or repeat offenses may result inpermanent blacklisting. Additionally, numbers which have been reported by industry partners for spam/unwanted content may also be subject to permanent blacklisting.
    b. Consumer: An individual person who subscribes to specific wireless messaging services or messaging applications. *Consumers do not include agents of businesses, organizations or entities which send messages to consumers*. Consumers are natural persons with uniquely assigned phone numbers (long codes i.e., local phone numbers) which can be dialed.
    c. Non-Consumer: A business, organization or entity which uses messaging to communicate with consumers. Examples may include, but are not limited to, large-to-small businesses, financial institutions, schools, medical practices, customer service entities, non-profit organizations, and political campaigns.
    d. Non-Consumer Application-to-Person (A2P): Messages sent from an application, typically web-based,to a mobile subscriber. Some common use cases include two-factor authentication (2FA), travel notifications, banking alerts or marketing messages. A2P delivery methods are either via toll-free messaging service or 10DLC (10-digit long code).
    e. Fingerprinting: The process of extracting data points from identified spam content is known as "fingerprinting". Once message content has been fingerprinted as spam, all content found to be correlated to that fingerprint will be blocked in the future. Fingerprints do not expire or age out of existence.
    f. MM4: MM4 is a 3GPP protocol for MMS service which covers the routing of an MMS from an originator MMS relay/server to a recipient MMS relay/server. MM4 is based on SMTP (email) protocol. MM4 is an extension of Internet simple mail transport protocol (SMTP) according to STD 10 (RFC 2821).
    g. Multimedia Message Service (MMS): Facilitates group messaging and allows for the exchange of multimedia content between mobile devices including video, pictures, and audio.
    h. REST API: Application programing interface (API) used to establish messaging connectivity for sendingand receiving messages and other service-related access.

i. Short Message Service (SMS): Commonly known as "text messaging" is a service for sending and receiving messages of up to 160 characters to mobile devices. Longer messages will be fragmented into smaller message fragments. Maximum character length per message fragment varies depending on the character set used in the body of the message, whether GSM default alphabet or Unicode.
j. Short Message Peer-to-Peer (SMPP): SMPP is an open, industry standard Internet protocol designed to provide a flexible data communication interface for the transfer of SMS messages between external short messaging entities (ESME), routing entities (RE) and short message service centers (SMSC).
k. Unwanted Messages: May include, but are not limited to, unsolicited bulk commercial messages (i.e., spam); "phishing" messages intended to access private or confidential information through deception; other forms of abusive, harmful, malicious, unlawful or otherwise inappropriate messages; and messages which require an opt-in but did not obtain such opt-in or such opt-in was revoked.

4. 10DLC and Toll Free:

a. 10DLC Registration & Toll Free Verification is mandatory for every 10DLC and/or toll free number that a customer purchases from or ports to BCM One for the purpose of Messaging. Customers using BCM One's Messaging services shall submit all required information necessary for, and assist BCM One personnel in, the successful completion of 10DLC Brand, 10DLC Campaign registrations and 10DLC-to-Campaign associations, as well as Toll Free Verifications.
b. Customers shall be liable for all costs related to 10DLC Registration, as well as Toll Free Verification, including all surcharges.

5. **General Rules of Content:** Message senders must take affirmative steps and employ tools which monitor and prevent unwanted message content, including content which:
   a. Is unlawful, harmful, abusive, malicious, misleading, harassing, violent, obscene/illicit, or defamatory
   b. Is deceptive (e.g., phishing messages intended to access private or confidential information), including deceptive links
   c. Invades privacy
   d. Causes safety concerns
   e. Incites harm, discrimination, hate or violence
   f. Intended to intimidate
   g. Includes malware
   h. Threatens consumers
   i. Does not meet age-gating requirements

6. **Political Use Cases**: Political messaging will be evaluated on a case-by-case basis. Such discretion will not be exercised with the intent of favor or disfavor of any political party or candidate. Due to high volumes of consumer complaints, messages containing the following content are not appropriate and may be blocked by carriers if sent over either P2P or A2P (toll-free/10DLC) messaging,regardless of opt-in status:
   a. Spoofing messages or snowshoed content across multiple numbers
   b. Data sharing between message senders
   c. Malicious content
   d. Phishing content

7. **Inappropriate Use Cases:** Due to high volumes of consumer complaints, messages containing the following content are not appropriate and may be blocked by carriers if sent over A2P (toll-free/10DLC) messaging, regardless of opt-in status. If messaging traffic is identified by a provider as associated with one of the following use cases, BCM One cannot do much to assist in the removal of blocking:
   a. Social marketing
   b. Collections
   c. Financial services, whether account notifications, marketing, collections or billing for:

d. High-risk/subprime lending/credit card companies
e. Auto loans
f. Mortgages
g. Payday loans
h. Short-term loans
i. Student loans
j. Debt consolidation/reduction/forgiveness
k. Insurance
l. Car Insurance
m. Health Insurance
n. Gambling, Casino, and Bingo
o. Gift cards
p. Sweepstakes
q. Free prizes
r. Investment opportunities
s. Lead generation
t. Recruiting
u. Commission programs
v. Credit repair
w. Tax relief
x. Illicit or illegal substances (including Cannabis)
y. Work from home
z. Get rich quick
aa. UGGS and RayBan campaigns
bb. Phishing
cc. Fraud or scams
dd. Cannabis
ee. Deceptive marketing
ff. SHAFT: Sex, Hate, Alcohol, Firearms or Tobacco

8. Additional Prohibited Practices:

a. Snowshoe Messaging: Snowshoe sending is a technique used to send messages from more source phone numbers or short codes than are needed to support an application's function. This technique is often used to dilute reputation metrics and evade filters. Message senders should not engage in snowshoe messaging. Service providers may also take measures to prevent snowshoe messaging. Certain cases with similar campaigns may use different numbers. In that case, it is important for message senders to identify their messages with a distinct brand and URL naming convention. If there isany doubt about campaign content, we suggest submitting use case proposals or questions to BCM One's messaging team.
b. Proxy Numbers: Message senders might utilize a phone number as a proxy number, which functions as a relay point between possibly large sets of phone numbers and/or frequently changing phone numbers in certain wireless messaging use cases. For example, a driver for a ride-sharing service may need to communicate with a prospective passenger to confirm a pick-up location. The proxy phone number functions as a conference call bridge phone number, allowing the driver and passenger to communicate without eitherparty having to reveal their personal phone number. A 10-digit NANP phone number used as a proxy is typically a means to connect two individuals, but proxy numbers are commonly reused in a way which may create volumes of messaging traffic exceeding typical consumer operation. Given the use of proxy numbers to facilitate bulk messaging traffic among multiple 10-digit NANP phone numbers, the proxy number qualifies as non-consumer (A2P) messaging traffic and may be subject to additional validation, vetting and monitoring.
c. Spoofing Phone Numbers: Message number spoofing includes the ability of a message sender to cause a message to display an originating number for the message, which is not assigned to the message sender,

or when a message sender originates a message through a service provider other than the service provider to which reply messages will be delivered or received. Message number spoofing should be avoided and should complywith all applicable laws.

d. Grey Routes: Message Senders should not utilize Grey Routes to send messages. A Grey Route is a setting, method or path that is not authorized by Service Providers for Non-Consumer (A2P) Messages. Messages are either Consumer (P2P) or Non-Consumer (A2P) in accordance with these Principles and Best Practices and subject to individual Service Providers' policies and arrangements.

9. Non-Consumer (A2P) Best Practices:

a. **Consumer Content:**

i. The messaging ecosystem should operate consistent with relevant laws and regulations, such as the TCPA and associated FCC regulations regarding consumer consent for communications. Regardless of whether these rules apply and to maintain consumer confidence in messaging services, non-consumer(A2P) message senders should:

1. Obtain a consumer's consent to receive messages generally
2. Obtain a consumer's express written consent to specifically receive marketing messages; and
3. Ensure consumers have the ability to revoke consent.

ii. Consent may vary upon on the type of message content exchanged with a consumer.

iii. The table in the following page provides examples of the types of messaging content and the associated consent that should be expected. The examples below do not constitute or convey legal advice and should not be used as a substitute for obtaining legal advice from qualified counsel. Reference to "business" below is used as an example of a non-consumer (A2P) message sender. Individual service providers may adopt additional consumer protection measures for non-consumer (A2P) message senders, which may include,for example, campaign pre-approval, service provider vetting, in-market audits, or unwanted message filtering practices which are tailored to facilitate the exchange of wanted messaging traffic.

Types of Messaging Content & Associated Consent Principles		
Conversational	Informational	Promotional
Conversational messaging is a back-and-forth conversation which takes place via text. If a Consumer texts a business first and the business responds quickly with a single message, then it is likely conversational. If the consumer initiates the conversation and the business simply responds, then no additional permission is expected.	Informational messaging is when a consumer gives their phone number to a business and asks to be contacted in the future. Appointment reminders, welcome texts, and alerts fall into this category because the first text sent by the business fulfills the consumer's request. A consumer needs to agree to receive texts for a specific informational purpose when they give the business their mobile number.	Promotional messaging is a message sent which contains a sales or marketing promotion. Adding a call-to-action (e.g., a coupon code to an informational text) may place the message in the promotional category. Before a business sends promotional messages, the consumer should agree in writing to receive promotional texts. Businesses which already ask consumers to sign forms or submit contact information can add a field to capture the consumer's consent.
First message is only sent by a consumer Two-way conversation	First message is sent by the consumer or business One-way alert or two-way conversation	First message is sent by the business One-way alert
Message responds to a specific request	Message contains information	Message promotes a brand, product, or service Prompts consumer to buy something, go somewhere, or otherwise take action
IMPLIED CONSENT If the consumer initiates the text message exchange and the business only responds to each consumer with relevant information, then no verbal or written permission is expected.	**EXPRESS CONSENT** The consumer should give express permission before a business sends them a text message. Consumers may give permission over text, on a form, on a website or verbally. Consumers may also give written permission.	**EXPRESS WRITTEN CONSENT** The consumer should give express written permission before a business sends them a text message. Consumers may sign a form, check a box online, or otherwise provide consent to receive promotional text messages.

b. Clear and Conspicuous Calls-to-Action:

i. A "call-to-action" is an invitation to a consumer to opt-in to a messaging campaign. The call-to-action for a single-message program can be simple. The primary purpose of disclosures is to ensure that a consumer consents to receive a message and understands the nature of the program. Message senders should display a clear and conspicuous call-to-action with appropriate disclosures to consumers about the type and purpose of the messaging consumers will receive. A call-to-action should ensure consumers are aware of:

1. The program or product description;
2. The phone number(s) or short code(s) from which messaging will originate;
3. The specific identity of the organization or individual being represented in the initial message;
4. Clear and conspicuous language about opt-in and any associated fees or charges; and
5. Other applicable terms and conditions (e.g., how to opt-out, customer care contact information and any applicable privacy policy).

ii. Calls-to-action and subsequent messaging should not contain any deceptive language, and opt-in details should not be obscured in terms and conditions (especially terms related to other services).

c. Consumer Opt-In:

i. Message senders should support opt-in mechanisms, and messages should be sent only after the consumer has opted-in to receive them. Opt-in procedures reduce the likelihood that a consumer will receive an unwanted message. It can also help prevent messages from being sent to a phone number which does not belong to the consumer who provided the phone number (e.g., a consumer purposefully or mistakenly provides an incorrect phone number to the message sender).

1. Depending upon the circumstances, a consumer might demonstrate opt-in consent to receive messaging traffic through several mechanisms, including but not limited to:
2. Entering a phone number through a website;
3. Clicking a button on a mobile webpage;
4. Sending a message from the consumer's mobile device that contains an advertising keyword;
5. Initiating the text message exchange in which the message sender replies to the consumer only with responsive information;
6. Signing up at a point-of-sale (POS) or other message sender on-site location; or
7. Opting-in over the phone using interactive voice response (IVR) technology.

ii. While the CTIA Short Code Monitoring Handbook (the "Handbook") is a separate document specific to the short code program, the Handbook has additional examples of opt-in consent which may behelpful to message senders. Message senders should also document opt-in consent by retaining the following data where applicable:

1. Timestamp of consent acquisition;
2. Consent acquisition medium (e.g., cell-submit form, physical sign-up form, SMS keyword, etc.);
3. Capture of experience (e.g., language and action) used to secure consent;
4. Specific campaign for which the opt-in was provided;
5. IP address used to grant consent;
6. Consumer phone number for which consent to receive messaging was granted; and
7. Identity of the individual who consented (name of the individual or other identifier (e.g., onlineusername, session ID, etc.)).

d. Confirm Opt-in Confirmation for Recurring Messages:

i. Message senders of recurring messaging campaigns should provide consumers with a confirmation message that clearly informs the consumer they are enrolled in the recurring message campaign and provides a clear and conspicuous description of how to opt-out. After the

message sender has confirmed that a consumer has opted-in, the message sender should send the consumer an opt-in confirmation message before any additional messaging is sent. The confirmation message should include:

1. The program name or product description;
2. Customer care contact information (e.g., a toll-free number, 10-digit phone number, or help command instructions);
3. How to opt-out;
4. A disclosure that the messages are recurring and the frequency of the messaging; and
5. Clear and conspicuous language about any associated fees or charges and how those chargeswill be billed.

e. **Consumer Re-Opt-in on Toll-Free Numbers**. A consumer may opt-in to a toll-free A2P campaign by texting the word "UNSTOP" to the sender's toll-free number. This keyword is not case sensitive and triggers opt-in only when sent as a single word. Examples of valid re-opt-ins:
    1. UNSTOP including variations such as unstop, Unstop or UNStop.
f. **Single Opt-in per Campaign**: Opt-ins are not transferrable. A consumer opt-in to receive messages should not be transferable or assignable. A consumer opt-in should apply only to the campaign(s) and specific message sender forwhich it was intended or obtained.
g. **Renting, Selling or Sharing Opt-in Lists.** Message senders should not use opt-in lists which have been rented, sold or shared to send messages. Message senders should create and vet their own opt-in lists.
h. **Consumer Opt-Out:**
    i. Opt-out mechanisms facilitate consumer choice to terminate messaging communications, regardless ofwhether consumers have consented to receive the message. Message senders should acknowledge andrespect consumers' opt-out requests consistent with the following:
        1. Message senders should ensure consumers have the ability to opt-out of receiving messages at any time;
        2. Message senders should support multiple mechanisms of opt-out, including phone call, email ortext; and
        3. Message senders should acknowledge and honor all consumer opt-out requests by sending onefinal opt-out confirmation message per campaign to notify the consumer that they have opted-out successfully. No further messages should be sent following the confirmation message.
        4. Message senders should state in the message how and what words effect an opt-out. Standardized "STOP" wording should be used for opt-out instructions, however opt-out requestswith normal language should also be read and acted upon by a message sender except where a specific word can result in unintentional opt-out. The validity of a consumer opt-out should not be impacted by any de minimis variances in the consumer opt-out response, such as capitalization, punctuation or any letter-case sensitivities.
    ii. Examples of valid opt-out messages:
        1. STOP including variations such as Stop or STop
        2. Quit
        3. Cancel
        4. Unsubscribe
        5. End
        6. Opt me out
i. **High opt-out Rate**. Message senders who receive high volumes of opt-outs could be flagged and indicative of poor sending practices. In the case that the daily opt-out rate is 5% or higher, the toll-free carrier or other carriers may monitor the campaign. The carrier may reach out for campaign and opt-in details and/or suspend services of high opt-out rate flagged campaigns at its discretion, not to be unreasonably exercised. "Daily opt-out rate" is the total number of subscribers who received a campaign's SMS divided by the number of opted out subscribers who received a campaign's SMS in a 24-hour period.

j. **Maintaining and Updating Consumer Information**. Message senders should retain and maintain all opt-in and opt-out requests in their records to ensure future messages are not attempted (in the case of an opt-out request) and consumer consent is honored to minimize unwanted messages. Message senders should process phone deactivation files regularly (e.g., daily) and remove any deactivated phone numbers from any opt-in lists.

k. **Privacy and Security**: Message senders should address both privacy and security comprehensively in the design and operationof messaging campaigns. BCM One is not responsible or liable for any security or breaches experiencedby the message sender.

   i. Maintain and Conspicuously Display a Clear, Easy-to-Understand Privacy Policy. Message senders should maintain and conspicuously display a privacy policy easily accessed by the consumer (e.g., through clearly labeled links) that clearly describes how the message sender may collect, use, and share information from consumers. All applicable privacy policies should be referenced in and accessible from the initial call-to-action. Message senders also should ensure that their privacy policy is consistent with applicable privacy law and their treatment of information is consistent with their privacy policy.

   ii. Implement Reasonable Physical, Administrative, and Technical SecurityControls to Protect and Secure Consumer Information. Message senders should implement reasonable security measures for messaging campaigns that include technical, physical, and administrative safeguards. Such safeguards should protect consumer information from unauthorized access, use, and disclosure. Message senders shouldconduct regular testing and monitoring to ensure such controls are functioning as intended.

   iii. Conduct Regular Security Audits. Message senders should conduct either a comprehensive self-assessment or third-party risk assessment of privacy and security procedures for messaging campaigns on a regular basis and takeappropriate action to address any reasonably foreseeable vulnerabilities or risks.

l. Content:

   i. Prevention of Unlawful Activities or Deceptive, Fraudulent, Unwanted or Illicit Content. Message senders should use reasonable efforts to prevent and combat unwanted or unlawful messaging traffic, including spam and unlawful spoofing. Specifically, message senders should takeaffirmative steps and employ tools to monitor and prevent unwanted messages and content, including for example content that: (1) is unlawful, harmful, abusive, malicious, misleading, harassing, excessively violent, obscene/illicit, or defamatory; (2) deceives or intends to deceive (e.g., phishing messages intended to access private or confidential information); (3) invades privacy; (4) causes safety concerns; (5) incites harm, discrimination, or violence; (6) is intended to intimidate; (7) includes malware; (8) threatens consumers; or (9) does not meet age-gating requirements. Message senders can also review the common short code handbook for further examples of unwanted message content. Further, message senders should take steps to ensure marketing content is not misleading and complies with the Federal Trade Commission's (FTC) Truth-In-Advertising rules.

   ii. Embedded Website Links. Message senders should ensure links to websites embedded within a message do not conceal or obscure the message sender's identity and are not intended to cause harm or deceive consumers. Where a web address (i.e., Uniform Resource Locator (URL)) shortener is used, message senders should use a shortener with a web address and IP address(es) dedicated to the exclusive use of themessage sender. Web addresses contained in messages as well as any websites to which they redirect should unambiguously identify the website owner (i.e., a person or legally registered business entity) and include contact information, such as a postal mailing address.

   iii. Embedded Phone Numbers. Messages should not contain phone numbers that are assigned to or forward to unpublished phonenumbers, unless the owner (i.e., a person or legally registered business entity) of such phone numbers is unambiguously indicated in the text message.

m. **Text-Enabling a Phone Number for Non-Consumer (A2P) Messaging**. An authentication and validation process should be used to verify the message senders' authorityto enable non-consumer (A2P) messaging for a specific phone number. Message senders should only enable non-consumer (A2P) messaging with a phone number that the message sender has been assigned by a provider of telecommunications or interconnected Voice over Internet Protocol(VoIP) services.

n. **Political Messaging.** Political campaigns should abide by the *M3AAWG Mobile Messaging Best Practices for Political Programs Best Practices*.

   i. T-Mobile Political Messaging. To run 10DLC messaging campaigns on the T-Mobile network, a special registration and third-partyverification check is required (Campaign Verify). This is required to ensure the authenticity of the political entity. Political candidates are required to send extended information that includes the following requirements:

      1. Campaign must be on a dedicated application address.
      2. 10DLC only: Vetting must be confirmed through Campaign Verify (www.campaignverify.org).
      3. Campaign Verify Token.
      4. FEC Committee ID.
      5. Politician/Organization Name.
      6. Politician/Organization Website

o. **A2P Toll-Free Messaging in Canada.** The Canadian market is continuing to evolve with regards to texting over A2P routes. Please reference our entire Best Practices for adherence on Canadian networks. Additionally, we have included the rules below, which should be followed.

   i. Opt-Out: Opt-out must be below 1%
   ii. Stop Language. Campaigns must send stop language on the first and 5th message or once a month for continued customer awareness. However, sending it on every message is recommended.
   iii. Single Number Sending. If a single number gets blocked with the Canadian carriers, please do not move traffic to another number.
   iv. Brand Identity. Messages should always identify who the sender of the message is.
   v. Message Frequency. The number of messages sent to a subscriber should not exceed 10 in a month. If there is an expectation that the subscriber will receive multiple messages, then that should be stated during the opt-in process.
   vi. Customer Support Keywords. Campaigns should support HELP, INFO and STOP as well as all French translations and send a bounce back in the corresponding language of the keyword.
   vii. False Positives. BCM One monitors on behalf of customers, but we encourage any issues to be reported to csp@skyswitch.com
   viii. Data Rates May Apply Verbiage. When a customer receives a message termination (MT) with a link to a website, messages must also state that "Data rates may apply."

10. **Resources.** The following industry resources may be helpful as a message sender starts to craft messaging content. Messages should follow guidance from these resources, otherwise messages may be blocked.

    a. CTIA Messaging Principles and Best Practices
    b. FTC Truth in Advertising
    c. MMA Best Practices
    d. M3AAWG Best Practices
    e. M3AAWG Mobile Messaging Best Practices for Political Programs
    f. Telephone Consumer Protection Act (TCPA) Omnibus Declaratory Ruling (FCC 15-72)